BE

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-036383

(43)Date of publication of application : 07.02.1995

(51)Int.Cl. G09C 5/00
G06K 7/10
G06K 17/00

(21)Application number : 05-315847

(22)Date of filing : 22.11.1993

(71)Applicant : PITNEY BOWES INC

(72)Inventor : MARCUS JAMES R

(30)Priority

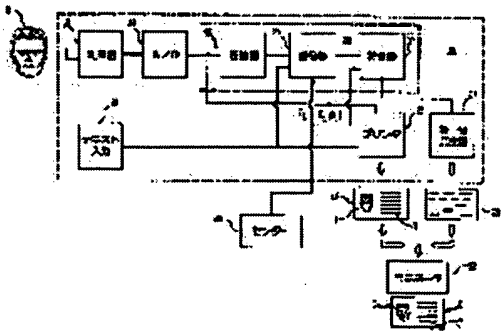
Priority number : 92 979018 Priority date : 20.11.1992 Priority country : US

(54) METHOD FOR IDENTIFYING OBJECT AND OTHER ENTITY AND DEVICE FOR MANUFACTURING IDENTIFICATION CARD

(57)Abstract:

PURPOSE: To obtain an identification card which is safe against alteration and forgery.

CONSTITUTION: A digital signal generated by scanning an entity to be certified by an dentification card, is compressed (16), enciphered (20), encoded as a two-dimensional bar code or the like (22), and integrated in the part of the identification card. A text message can be added to a signal before encoding (30), and the text message can also be printed in the identification card as a sentence. For example, a signal indicating a an image is enciphered by using a public key encipherment system, and the key is always changed for improving safety. A corresponding decoding key is enciphered by another key, and integrated into the card for easily attaining certification. The encoded message is scanned, decoded, extended, displayed, and compared with the image and text message printed in the card for confirming the validity of the card so that the card can be certified.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平7－36383

(43)公開日　平成７年(1995)２月７日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ　5/00		8837－5L		
Ｇ０６Ｋ　7/10		P 9191－5L		
17/00		V		

審査請求　未請求　請求項の数47　ＦＤ　（全 8 頁）

(21)出願番号　特願平5－315847

(22)出願日　平成５年(1993)11月22日

(31)優先権主張番号　９７９０１８

(32)優先日　1992年11月20日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591142781
ピットニー、ボウズ、インコーポレーテッド
ＰＩＴＮＥＹ　ＢＯＷＥＳ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国コネチカット州、スタムフォード　（番地なし）

(72)発明者　ジェームズ、アール、マーカス
アメリカ合衆国コネチカット州、ノーウォーク、ブロード、コート、１

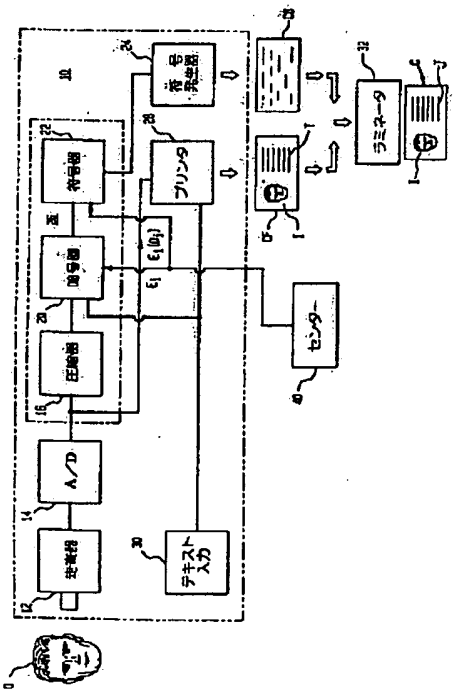
(74)代理人　弁理士　佐藤　一雄　（外３名）

(54)【発明の名称】　物その他の実体を識別する方法および識別カードを製造する装置

(57)【要約】　（修正有）

【目的】　変造および偽造に対して安全である識別カードを得る。

【構成】　識別カードが証明する実体を走査して発生したデジタル信号を圧縮し、暗号化し、二次元バーコード等として符号化し、識別カードの部分に組み込む。暗号化される前の信号にテキスト・メッセージを付すことができ、かつそのテキスト・メッセージを平文で識別カードにプリントすることもできる。例えば、画像を表す信号が公開鍵暗号方式を用いて暗号化され、安全性を高くするために鍵は始終変更される。認証を容易にするために対応する解読鍵は別の鍵により暗号化されてカードに組み込まれる。カードの有効性を確認するために符号化されたメッセージが走査され、復号され、解読され、拡張され、表示され、カードにプリントされている画像及びテキスト・メッセージと比較することによりカードを認証できる。



1

【特許請求の範囲】

【請求項1】 a）物その他の実体を走査して、その物その他の実体の画像を表す第1の信号を発生する過程と、

b）前記画像を識別カードの第1の部分の上にプリントする過程と、

c）前記画像の表現を含み、前記第1の信号から少なくとも部分的に得られる第2の信号を暗号化する過程と、

d）前記暗号化された第2の信号の符号化された表現を前記識別カードの第2の部分に組み込む過程と、

e）前記第2の信号の前記符号化された表現を前記識別カードから読出す過程と、

f）前記第2の信号を復号する過程と、

g）前記復号された第2の信号を解読する過程と、

h）前記画像の前記表現を表示するために前記解読された第2の信号を表示装置へ入力する過程と、

i）前記プリントされた画像を前記表示された第2の画像と比較して前記カードの有効性を確認する過程と、

j）前記プリントされた画像を前記物その他の実体と比較してそれの同一性を確認する過程と、を備える物その他の実体を識別する方法。

【請求項2】 請求項1記載の方法において、前記第1の信号をデジタル信号へ変換する過程を更に備える方法。

【請求項3】 請求項2記載の方法において、前記第2の信号は圧縮された態様の前記第1の信号を含む方法。

【請求項4】 請求項3記載の方法において、公開鍵暗号化システムに対する暗号化鍵、E_i、を用いて前記第2の信号を暗号化する方法。

【請求項5】 請求項4記載の方法において、前記暗号化鍵、E_i、に対応する解読鍵、D_i、を、前記公開鍵暗号化システムに対する第2の暗号化鍵、E_i、で暗号化する方法。

【請求項6】 請求項5記載の方法において、前記暗号化された解読鍵、E_i［D_i］を、前記第2の部分に組み込む前に、前記暗号化された第2の信号へ付す方法。

【請求項7】 請求項6記載の方法において、前記暗号化された第2の信号の前記表現を二次元バーコードとして前記第2の部分中に組み込む方法。

【請求項8】 請求項6記載の方法において、前記暗号化された第2の信号の解読は、解読鍵D_iを用いて前記暗号化された鍵、E_i［D_i］を解読する過程を更に備える方法。

【請求項9】 請求項3記載の方法において、前記暗号化された第2の信号の前記表現を二次元バーコードとして前記第2の部分中に組み込む方法。

【請求項10】 請求項2記載の方法において、前記第2の信号はテキスト・メッセージを備える方法。

【請求項11】 請求項10記載の方法において、前記物その他の実体は人であり、前記テキスト・メッセージはその人が知っている暗証である方法。

【請求項12】 請求項10記載の方法において、前記テキスト・メッセージを平文テキスト形式で前記識別カードの前記第1の部分にプリントする方法。

2

【請求項13】 a）物その他の実体を走査して前記物その他の実体の画像を表す第1の信号を生ずる過程と、

b）前記画像を前記カードの第1の部分の上にプリントする過程と、

c）前記画像の表現を含み、前記第1の信号から少なくとも部分的に得られる第2の信号を暗号化する過程と、

d）前記暗号化された第2の信号の符号化された表現を前記識別カードの第2の部分中に組み込む過程と、を備える識別カードを製造する方法。

【請求項14】 請求項13記載の方法において、前記第1の信号をデジタル信号へ変換する過程を更に備える方法。

【請求項15】 請求項14記載の方法において、前記第2の信号は圧縮された態様の前記第1の信号を含む方法。

【請求項16】 請求項15記載の方法において、公開鍵暗号化システムに対する暗号化鍵、E_i、を用いて前記第2の信号を暗号化する方法。

【請求項17】 請求項16記載の方法において、前記暗号化鍵、E_i、に対応する解読鍵、D_i、を、前記公開鍵暗号化システムに対する第2の暗号化鍵、E_i、で暗号化する方法。

【請求項18】 請求項17記載の方法において、前記暗号化された解読鍵、E_i［D_i］を、前記第2の部分に組み込む前に、前記暗号化された第2の信号へ付す方法。

【請求項19】 請求項18記載の方法において、前記暗号化された第2の信号の前記表現を二次元バーコードとして前記第2の部分に組み込む方法。

【請求項20】 請求項15記載の方法において、前記暗号化された第2の信号の前記表現を二次元バーコードとして前記第2の部分に組み込む方法。

【請求項21】 請求項14記載の方法において、前記第2の信号はテキスト・メッセージを備える方法。

【請求項22】 請求項21記載の方法において、前記物その他の実体は人であり、前記テキスト・メッセージはその人が知っている暗証である方法。

【請求項23】 請求項21記載の方法において、前記テキスト・メッセージを平文テキスト形式で前記識別カードの前記第1の部分にプリントする方法。

【請求項24】 a）識別カードにより識別すべき物その他の実体の画像を発生するための走査手段と、

b）この走査手段に応答して前記画像を前記識別カードの第1の部分にプリントするプリント手段と、

c）前記画像の表現を含み、前記第1の信号から少なくとも部分的に得られる第2の信号を暗号化する暗号化手段と、

d）前記第2の信号の前記暗号化の符号化された表現を

3

前記識別カードの第２の部分に組み込む符号化手段と、を備える識別カードを製造する装置。

【請求項２５】請求項２４記載の装置において、前記第１の信号をデジタル信号へ変換するアナログーデジタル変換器を更に備える装置。

【請求項２６】請求項２５記載の装置において、前記第１の信号を圧縮する手段を更に備える装置。

【請求項２７】請求項２５記載の装置において、公開鍵暗号化システムに対する暗号化鍵、E_1、を用いて前記第２の信号を暗号化する手段を更に備える装置。

【請求項２８】請求項２７記載の装置において、解読鍵、D_1、が第２の暗号化鍵、E_1、で暗号化され、暗号化された解読鍵、E_1［D_1］が、前記第２の部分に組み込まれる前に、前記暗号化された第２の信号へ付される装置。

【請求項２９】請求項２７記載の装置において、前記暗号化された第２の信号の前記表現を二次元バーコードとして前記第２の部分に組み込む手段を更に備える装置。

【請求項３０】請求項２７記載の装置において、前記暗号化鍵、E_1、と前記暗号化された解読鍵、E_1［D_1］を中央局から受ける手段を更に備える装置。

【請求項３１】請求項２６記載の装置において、前記暗号化された第２の信号の前記表現を二次元バーコードとして前記第２の部分に組み込む手段を更に備える装置。

【請求項３２】識別すべき物その他の実体の画像を第１の部分の上に有し、組み込まれた前記画像の符号化された表現を第２の部分の上に有する識別カードの有効性を確認する方法であって、

a）前記信号の前記符号化された表現を前記カードから読出す過程と、

b）前記信号の前記符号化された表現を復号する過程と、

c）前記信号の前記暗号化された表現を解読する過程と、

d）前記画像の前記表現を表示するための表示器へ前記信号の前記解読された表現を入力する過程と、を備え、それにより、

e）前記カードの前記第１の部分における前記画像を、前記画像の表示された表現と比較することにより前記カードの有効性を確認できる識別カードの有効性を確認する方法。

【請求項３３】請求項３２記載の方法において、公開鍵暗号化システムに対する暗号化鍵、E_1、を用いて前記暗号化された信号を暗号化する方法。

【請求項３４】請求項３３記載の方法において、前記鍵、E_1、に対応する解読鍵、D_1、を、前記公開鍵暗号化システムに対する第２の暗号化鍵、E_1、で暗号し、前記暗号化された解読鍵、E_1［D_1］を前記暗号化された信号へ付し、前記解読過程は、

a）前記暗号化された解読鍵、E_1［D_1］を対応する

4

解読鍵D_1で解読して前記解読鍵、D_1、を回復する過程と、

b）前記暗号化された信号を前記鍵、D_1、で解読する過程と、を備える方法。

【請求項３５】識別すべき物その他の実体の画像を第１の部分に有し、組み込まれた前記画像の符号化された表現を第２の部分の上に有する識別カードの有効性を確認する装置であって、

a）前記信号の前記符号化された表現を前記カードから読出す手段と、

b）この読出し手段に応答して、前記信号の前記符号化された表現を復号する復号手段と、

c）この復号手段に応答して、前記信号の前記復号された表現を解読する解読手段と、

d）この解読手段に応答して、前記画像の前記表現を表示する表示手段と、を備え、それにより、

e）前記カードの前記第１の部分における前記画像を、前記画像の表示された表現と比較することにより前記カードの有効性を確認できる識別カードの有効性を確認する装置。

【請求項３６】請求項３５記載の装置において、公開鍵暗号化システムに対する暗号化鍵、E_1、を用いて前記暗号化された信号が暗号化される装置。

【請求項３７】請求項３６記載の装置において、前記鍵、E_1、に対応する解読鍵、D_1、が、前記公開鍵暗号化システムに対する暗号化鍵E_1で暗号化されて、暗号化された解読鍵、E_1［D_1］を形成し、前記暗号化された解読鍵、E_1［D_1］を前記暗号化された信号へ付し、前記解読手段は、

a）前記暗号化された解読鍵、E_1［D_1］を対応する解読鍵D_1で解読して前記解読鍵、D_1、を回復する手段と、

b）前記暗号化された信号を前記鍵、D_1、で解読する手段と、を備える装置。

【請求項３８】識別カードであって、この識別カードは、

a）前記識別カードにより識別すべき物その他の実態の画像を有する第１の部分と、

b）前記画像の表現を含む暗号化された信号の符号化された表現を組み込む第２の部分と、を備える識別カード。

【請求項３９】請求項３８記載の識別カードにおいて、前記信号はデジタル信号である識別カード。

【請求項４０】請求項３９記載の識別カードにおいて、前記デジタル信号は、前記物その他の実態を走査することにより発生された走査信号から得られる圧縮された信号を備える識別カード。

【請求項４１】請求項４０記載の識別カードにおいて、公開鍵暗号化システムに対する暗号化鍵、E_1、を用いて前記デジタル信号が暗号化される識別カード。

5

【請求項４２】請求項４１記載の識別カードにおいて、前記暗号化鍵、E_1、に対応する解読鍵、D_1、が、前記公開鍵暗号化システムに対する暗号化鍵E_1で暗号化されて、暗号化された解読鍵、E_1［D_1］を形成し、前記暗号化された解読鍵、E_1［D_1］は、前記第２の部分へ組み込む前に、前記デジタル信号へ付される識別カード。

【請求項４３】請求項４２記載の識別カードにおいて、前記暗号化されたデジタル信号の前記表現は二次元バーコードとして前記第２の部分に組み込まれる識別カード。

【請求項４４】請求項４０記載の識別カードにおいて、前記暗号化されたデジタル信号は二次元バーコードとして前記第２の部分に組み込まれる識別カード。

【請求項４５】請求項３９記載の識別カードにおいて、前記デジタル信号はテキスト・メッセージを備える識別カード方法。

【請求項４６】請求項４５記載の識別カードにおいて、前記物その他の実体は人であり、前記テキスト・メッセージはその人が知っている暗証である識別カード。

【請求項４７】請求項４５記載の識別カードにおいて、前記テキスト・メッセージは前記識別カードの前記第１の部分の上の平文テキスト形式である識別カード。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、物その他の実体の同一性または状態の証拠として機能する識別カードまたはそれに類似の物品に関するものである。更に詳しく言えば、本発明は、偽造または変造に対して高度の安全性を有する識別カードまたは類似の物品と、それらのカードの製造及び認証方法および装置に関するものである。

【０００２】（この明細書で使用する「識別カード」という用語は、従業員を識別するために事業所により用いられる種類の識別バッジに類似する物を指すものであるが、文書、磁気ディスク、ＣＤ等、または関連するデータと共に画像を記録でき、かつ識別すべき物その他の実体に関連させることができるその他の任意の適当な物を、ここで使用する「識別カード」という用語が限定なしに含むべきことが、本発明の意図に含まれる。）物その他の実体の識別は少なくとも歴史のように古い問題である。年取って盲目になったイサクは、エサウの相続権に頼ってエサウをヤコブから見分けることに失敗し、ソロモンは赤子の母親を見つけるためにその赤子を殺すと脅かす事を余儀なくされた。歴史および物語は、所持している人を識別するために用いられる手紙、しるし、玉璽および暗証と、それらが失われ、または偽造された後に続く結末についての話に満ちている。

【０００３】現代においては、この問題についての最もありふれた解決は、所有者の同一性と、所有者の通常はある特徴、状態、または属性を定める機能を果たす識別

6

カードである。それの例は上記のように従業員バッジであり、最も一般的には運転免許証である。典型的には、そのような識別カードは公称所有者の写真と、文書形式の関連する情報とを含む。

【０００４】識別カードなどは毎日の管理業務に有用であることが一般に判明しているが、それでも、識別カードは偽造または変造されることがあり、偽の識別文書を供給する目的の適度な規模の非合法事業が存在する。

【０００５】識別についての高度の安全性が要求される用途に対しては、指紋、声紋、網膜模様、その他の個人的な特徴を認識するための効率的な技術が開発されている。そのようなシステムはシステムが知っている個人を一意に識別するのには極めて成功しているが、選択された個人を指紋のような身体的特徴で識別するデータベースへ接続せねばならない、典型的には可動ではない、極めて高性能の、極めて高価なセンサを必要とすることが欠点である。不法な変更に対する保護と更新を容易にするために、そのようなデータベースは一般に中央に設置せねばならない。したがって、それらの高度なシステムは区域を安全にするために接近を制約することに一般に限定される。

【０００６】以上の説明から明らかなように、識別カードの最も一般的な用途は個人識別である。しかし、識別の目的は非常に広い種類の物その他の実体に拡張できる。したがって、特定の項目が検査された、または税関を通過した、あるいは特定の会社により製造された、ことを確証できることが望ましい。同様に、美術工芸品の出所、動物の血統または人の家系、あるいは植物が病原菌に犯されていないこと、の確実な証拠を持つことが望ましい。そのような用途、および当業者には明らかであるその他の用途は本発明の範囲内である。

【０００７】おそらく有体物ではなくて情報に関連するからであろう、文書その他の態様の情報の識別すなわち認証が過去において、通常はある種の暗号化を使用することにより、多分成功裡に取り扱われてきた。したがって、１９８９年８月１日にパストー（Ｐａｓｔｏｒ）へ付与された米国特許第４，８５３，９６１号「信頼できる文書認証装置（Ｒｅｌｉａｂｌｅ Ｄｏｃｕｍｅｎｔ Ａｕｔｈｅｎｉｃａｔｉｏｎ Ｓｙｓｔｅｍ）」には、公開鍵暗号方式を用いる暗号化により文書を認証する装置が開示されている。クラーク（Ｃｌａｒｋ）へ付与された米国特許第４，６３７，０５１号には、暗号化により認証される標識を持つ郵便料金計が開示されている。情報を認証するための暗号化のその他の多くの用途が当業者には知られていることであろう。

【０００８】

【発明が解決しようとする課題】したがって、本発明の目的は、変造および偽造に対して安全である、物その他の実体を識別するための識別カードを得ることである。

【０００９】

【課題を解決するための手段】識別カードを製造する方法および装置、およびその識別カードの有効性を確認する方法および装置を提供する本発明により上記目的は達成され、かつ従来技術の諸欠点が克服される。識別カードを製造する装置は、識別すべき物その他の実体の画像を表す第１の信号を発生する走査器と、この走査器に応答して画像を識別カードの第１の部分の上にプリントするプリンタとを含む。この装置は、画像の表現を含み、第１の信号から少なくとも部分的に得られる第２の信号を暗号化する暗号化器と、第２の信号の暗号化の符号化された表現を識別カードの第２の部分に組み込む符号器とを更に含む。

【００１０】そのようにして製造された識別カードの有効性を確認する装置は、第２の信号の符号化された表現をカードから読出す読出し器と、この読出し器の第２の信号の符号化された表現を復号する復号器と、復号された表現を解読する解読器と、第２の信号に組み込まれている画像の表現を表示する表示器とを含む。

【００１１】本発明の方法に従って、識別すべき物が走査されて第１の信号を発生し、第１の信号により制御されるプリンタがその物の画像を識別カードの第１の部分の上にプリントする。第１の信号から少なくとも部分的に得られ、画像の表現を含む第２の信号を暗号化および符号化し、識別カードの第２の部分に組み込む。

【００１２】ひとたび製造されたカードは、第２の信号の符号化された表現を識別カードから読出し、解読された第２の信号に従って表示装置を制御して、第２の信号に含まれている画像の表現を表示する。それから画像の表示された表現およびカードの第１の部分にプリントされた画像を物と比較してそれの同一性を確認する。

【００１３】本発明の１つの面に従って、第１の信号は処理のためにデジタル信号へ変換される。

【００１４】本発明の別の面に従って、第２の信号は圧縮された態様の第１の信号を含む。

【００１５】（信号圧縮は当業者に周知であって、デジタル信号の場合には、伝送または処理せねばならないバイト数を減少し、しかもその信号により表されている情報のほとんど全てを依然として保持するために、信号に対する所定のアルゴリズムの適用を含む。）本発明の別の面に従って、第２の信号は公開鍵暗号化システムに対する暗号化鍵E_1を用いて暗号化される。

【００１６】本発明の別の面に従って、暗号化鍵、E_1、に対応する解読鍵、D_1、を、公開鍵暗号化システムに対する第２の暗号化鍵、E_1、で暗号化し、結果としての暗号化された解読鍵、E_1［D_1］を、第２の部分に組み込む前に、暗号化された第２の信号へ付す。

【００１７】本発明の別の面に従って、暗号化された第２の信号を二次元バーコードとして識別カードの第２の部分にプリントする。

【００１８】本発明の別の面に従って、識別カードの有効性を識別する装置は鍵E_1に対応する解読鍵、D_1を記憶し、暗号化された第２の信号の解読は、暗号化された解読鍵、E_1［D_1］を、解読鍵、D_1を用いて解読して解読鍵D_1を得、それから暗号化された第２の信号をその解読鍵を用いて解読する過程を含む。

【００１９】本発明の別の面に従って、第２の信号はテキスト・メッセージを含み、そのテキスト・メッセージは識別カードにより識別すべき人が知っている暗証を含む。

【００２０】本発明の更に別の面に従って、第２の信号はテキスト・メッセージを含み、そのテキスト・メッセージは識別カードの第１の部分に平文形式でプリントもされる。

【００２１】したがって、本発明は、同一性を確認すべき物その他の実体と容易に比較でき、かつ偽造または変造に強い画像を含む識別カードを製造する方法および装置により、上記目的を達成するものであることがわかる。

【００２２】

【実施例】図１は識別カードＣを製造するための装置１０の概略ブロック図を示す。識別カードが意図されている人（または物その他の実体）が通常のテレビカメラ１２により走査されて、その人の画像を表す第１の信号を発生する。それから、第１の信号をデジタル領域で処理するためにアナログーデジタル変換器１４によりデジタル形式へ変換することが好ましい。しかし、以下に説明する少なくとも信号圧縮技術および暗号化技術を、アナログ信号処理技術における当業者に周知の信号圧縮技術および信号暗号化技術を用いてアナログ領域において実施できる。

【００２３】それから、第１の信号は圧縮モジュール１６へ入力され、そこで圧縮されて、識別カードに記憶せねばならないデータの量を減少する。

【００２４】カードＣが現在知られている識別カード、運転免許症などとほぼ同じ形式を持つ場合には、現在の技術状態においてはデータ圧縮を必要とすることに注目すべきである。しかし、データ記憶技術における予測される改良により、または識別カードが高い容量の記憶媒体（たとえば、フロッピーディスク）を含むことができる用途においては、後で述べるように第１の信号を圧縮する必要がないが、完全な信号を処理できることも本発明の範囲内である。

【００２５】データ圧縮アルゴリズム、とくにビデオ画像信号の圧縮に用いられるデータ圧縮アルゴリズム、は当業者に周知である。市販されているＪＰＥＧアルゴリズムとして知られているアルゴリズムを圧縮器１６に用いることが好ましい。圧縮器１６の動作の動作についてのこれ以上の説明は本発明の理解には不必要であると信ぜられる。

【００２６】それから圧縮された第１の信号は暗号器２

０へ入力されて、暗号化された第２の信号に含まれる。その暗号化された第２の信号は、後で説明するように、識別カードＣに組み込まれる。暗号器２０は周知のＲＳＡ方式のような公開鍵暗号方式のための暗号化鍵、E_1、を用いて第２の信号を暗号化することが好ましい。

【００２７】それから暗号化された第２の信号は符号器モジュール２２によりある所定のフォーマットに従って符号化される。それは符号発生器２４を制御して符号化されて暗号化された第２の信号を識別カードＣの部分中に組み込ませる。

【００２８】本発明の好適な実施例に従って、符号化された信号は、ニューヨーク所在のシンボル・テクノロジー・コーポレーション（Ｓｙｍｂｏｌ　Ｔｅｃｈｎｏｌｏｇｙ　Ｃｏｒｐｏｒａｔｉｏｎ）により開発されたＰＤＦ－４１７標準バーコードのような、二次元バーコードとして符号化される。しかし、暗号化された第２の信号は適当な任意のフォーマットへ符号化できる。たとえば、スマートカードまたは記憶カードに対して符号器２２およびコード発生器２４は符号化された第２の信号を適切にフォーマット化された２進データ・ブロックとして記憶できる。

【００２９】符号化された第２の信号が二次元バーコードとして表される好適な実施例においては、バーコードは識別カードＣの裏ＣＢにプリントすることが好ましい。

【００３０】本発明の好適な実施例においては、圧縮器モジュール１６と、暗号器モジュール２０と、符号器モジュール２２とはマイクロプロセッサにおけるソフトウエア・モジュールとして実現される。そのマイクロプロセッサはインテル８０３８６型、またはそれと同等品、あるいはより高い性能のマイクロプロセッサであることが好ましい。

【００３１】デジタル化された第１の信号はプリンタ２０へも入力される。そのプリンタは、人Ｏの画像を識別カードＣの表面ＣＦにプリントするために識別カードＣを製造する任意の適切な技術を使用できる。それから表面ＣＦと裏面ＣＢを組合わせ、ラミネータ３２により周知の技術を用いてラミネートして識別カードＣを製造する。

【００３２】本発明の別の好適な実施例に従って、テキスト・メッセージを入力するためにテキスト入力部３０が用いられる。本発明の一実施例においては、テキスト・メッセージの少なくとも一部が圧縮された態様の第１の信号に組合わされて第２の信号を形成する。その第２の信号は暗号器モジュール２０により暗号化され、かつカードＣの表面ＣＦに平文テキストとしてプリントもされる。あるいは、テキスト・メッセージＴを、たとえば、制御キャラクタの削除により圧縮できる。それらのキャラクタは、テキスト・メッセージＴが第２の信号へ組み込まれる前に、テキストＴが回収された時に、所定のフォーマットに従って回復される。したがって、画像Ｉのようにテキスト・メッセージＴは、カードＣの表面ＣＦに人が認識できる形式で、および裏面ＣＢに符号化された形式でカードＣに具体化される。別の実施例においては、テキスト・メッセージは暗証Ｐを含むことができる。その暗証は暗号化され、かつ符号化されるが、表面ＣＦには平文でプリントされない。

【００３３】本発明の好適な実施例においては、センター４０が暗号化鍵E_1を暗号器モジュール２０へ送る。識別カードＣの安全性を高くするために、鍵E_1を始終変更する。鍵E_1の安全度を最高にするためには、各カードＣを製造するたびに鍵を変更し、または第２の信号の種々の部分を暗号化するために異なる鍵を使用することもできる。

【００３４】鍵E_1がしばしば変更される環境における第２の信号の暗号化を容易にするために、センター４０は暗号化された解読鍵E_1［D_1］を送って符号器モジュール２２により暗号化された第２の信号へ付させる。このように、下でわかるように、カードＣの有効性を確認する時に、E_1［D_1］を解読することにより必要な解読鍵D_1を得ることができる。

【００３５】典型的には、暗号化鍵／解読鍵対E_1、D_1は装置１０が動作中はほぼ一定のままである。しかし、各種の組織のための識別カードＣを製造するために装置１０が使用される用途においては、種々の鍵対E_1、D_1を種々の組織のために使用できる。

【００３６】次に、識別カードＣの有効性を確認するための装置５０が示されている図２を参照する。カードＣの裏面ＣＢが、適切な二次元バーコードを走査できる性能を有するバーコード走査器５２により走査される。本発明の好適な実施例においては、解読鍵D_1を得るために暗号化されている解読鍵E_1［D_1］を解読するために用いられる解読鍵D_1を解読器５８が保存する。それから鍵D_1を用いて、カードの裏面ＣＢから走査される復号された信号を解読する。

【００３７】鍵D_1はセンター４０から解読器５８により得られる。典型的には、上記のように、装置５０の動作中は鍵D_1は一定に保たれ、装置５０とセンター４０の間の直接通信リンクは不必要であり、鍵D_1は任意の便利なやり方で送ることができる。しかし、識別カードＣが所定の満期期限を有するある用途においては、その満期期限の経過後は鍵D_1を変更することが望ましく、そのような満期期限が十分にしばしば生ずるものとすると、センター４０への直接通信リンクを装置５０に含むことができる。

【００３８】それから、解読された走査信号は装置１０において使用される圧縮アルゴリズムに対して相補的なアルゴリズムにより、通常のやり方で拡張される。本発明の理解のためにはそのやり方を説明する必要はない。

11

【００３９】本発明の好適な実施例においては、復号器モジュール５４と、解読器モジュール５８と、拡張器モジュール６０とをマイクロプロセッサ６１においてソフトウエア・モジュールとして実現できる。

【００４０】解読され、拡張された信号がそれから通常の表示装置６２により表示される。表示装置は画像Ｔの表現ＲＩと、カードの裏面ＣＢから走査される暗号化された第２の信号に含まれていたテキスト・メッセージＴとを含む。表示装置は暗証Ｐ１含む。その暗証はカードＣを所持することを許されている人Ｏに知られているが、上記のようにカードＣには含まれない。カードの有効性を確認するために、画像Ｉがそれの表現ＲＩと比較され、カードＣにプリントされていて、表示装置６２に示されているテキスト・メッセージＴが比較される。圧縮により表現ＲＩが画像Ｉに対して多少劣化させられることに注目すべきである。しかし、上記ＪＰＥＧアルゴリズムを使用すると、人の顔の画像の十分に正確な表現をデータの約１０００バイトとして符号化でき、ほぼ従来の札入れ寸法のカードの裏面に約６．３５×４．４５ｃｍ（約２．５０×１．７５インチ）の区域に上記ＰＤＦ－４１７二次元バーコードを用いてプリントできる。もちろん、上記のように、記憶装置技術の改良と、より大きいデータ記憶容量を有する媒体の使用との少なくとも一方により、識別カードＣの表現ＲＩの実施例を画像Ｉへ任意に近づけることができる。

【００４１】暗証Ｐを含む実施例においては、暗証Ｐは表示装置６２の上に示されるが、カードの表面ＣＦにはもちろんプリントされない。暗証ＰはカードＣを所持する事を許されている人Ｏは知っている。画像Ｉと、カードの表面ＣＦにプリントされているテキスト・メッセージＴを、表示装置６２に示されている表現ＲＩとテキスト・メッセージＴと比較することにより有効であることが確認されると、カードＣを所持している人Ｏと画像Ｉを比較し、かつ暗証Ｐを知っているかどうかその人Ｏを試すことにより、その人を確認できる。それからテキスト・メッセージＴはその人Ｏの同一性を確認し、かつその人Ｏの状態または特徴も確認できる。

12

【図面の簡単な説明】

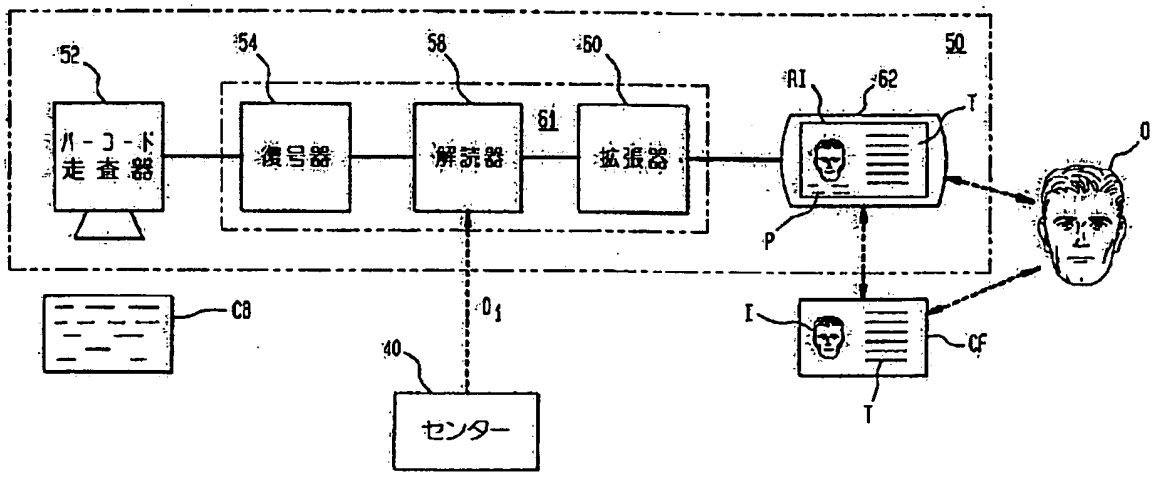
【図１】本発明に従って識別カードを製造する装置の概略ブロック図である。

【図２】本発明に従って製造された識別カードの有効性を確認する装置の概略ブロック図である。

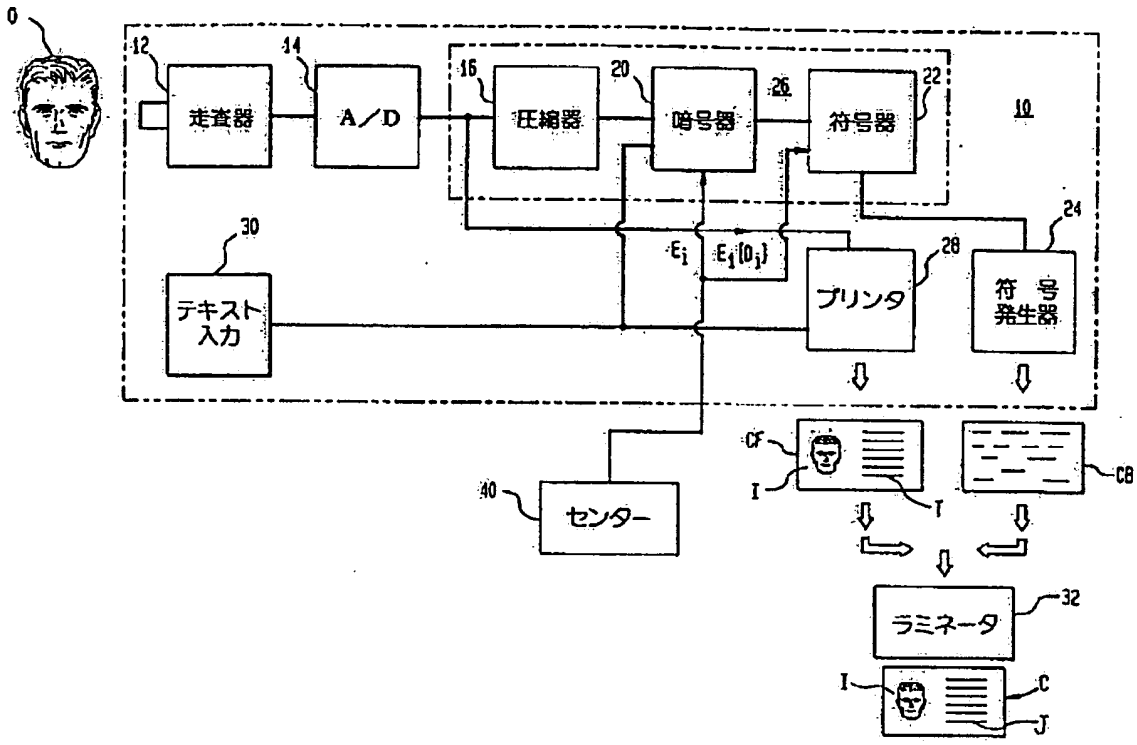
【符号の説明】

１０　識別カードを製造する装置
１２　走査器
１４　アナログーデジタル変換器
１６　圧縮器
２０　暗号器
２２　符号器
２４　符号発生器
２８　プリンタ
３０　テキスト入力部
３２　ラミネータ
４６　センター
５０　識別カードの有効性を確認する装置
５２　バーコード走査器
５４　復号器
５８　解読器
６０　拡張器
６１　マイクロプロセッサ
６２　表示装置

【図２】



【図1】


0
12
走査器
14
A／D
16
圧縮器
20
暗号器
26
符号器
22
10
24
30
テキスト入力
E_i
$E_i(D_j)$
プリンタ
28
符号発生器
CF
I
I
CB
40
センター
ラミネータ
32
I
C
J